Intentional Electromagnetic Interference Effects in Cyber-Physical Systems

J F Dawson:
Department of Electronics, University of York

ABSTRACT

This paper gives an overview of the possible effects of Intentional Electromagnetic Interference (IEMI) on Cyber-Physical systems. Examples of a range of attacks and possible countermeasures are presented.

INTRODUCTION

A cyber-physical system (CPS) is a system of collaborating computational elements controlling physical entities [1]. We are experiencing a world where much of our everyday life is becoming dependent on cyber-physical systems. Examples extend from home appliances, to transport, factories, and the utility infrastructure which supplies water, power, etc. The possible use of Intentional Electromagnetic Interference (IEMI) to disrupt critical systems is becoming a significant concern [2]. A failure due to IEMI may be blamed on faulty hardware or software, and much time and money may be wasted on searching for the cause, particularly if the failure is intermittent. It is also possible that false information can be injected into systems causing erroneous operation which may not be detected until sometime later.

This paper outlines possible intentional interference mechanisms and provides some examples of attacks on specific systems and countermeasures that can be applied.

INTERFERENCE WITH COMMUNICATION, RADAR, AND NAVIGATION SYSTEMS

Radio communications, radar, and navigation systems rely on the propagation of electromagnetic waves which have a low amplitude at the receive antenna due to attenuation in the propagation path and the practical limits to transmit power. It is therefore possible to interfere with the information transmitted by: jamming to prevent the communications; or by injecting false information (spoofing). Fields of sufficient intensity can also cause permanent damage to the sensitive receiver front-end.

We are increasingly relying on wireless connectivity for systems ranging from sensor networks in the internet of things (IoT), machine-to-machine (M2M) communications in factories, warehouses, and in critical infrastructure. Aircraft, shipping, and autonomous vehicles of all kind rely on radar, navigations systems, and communication system. All of these are vulnerable to intentional electromagnetic interference. A best interference may cause some inconvenience, at worst it could cause serious failures resulting in economic losses, death and injury.

Jamming and spoofing are two common interference types. Jamming can be achieved with simple, low power equipment. If the source can be placed near the receiver, it can be of a much lower power output than the original transmitter. Jamming is therefore difficult to prevent, though potentially easy to detect. Spoofing, replacing an authentic signal with a false one, requires more sophisticated equipment than jamming but has the potential to cause much greater problems as false data can be fed into a system. Detection of spoofing is possible using cryptographic methods to protect and identify valid data.

Jamming and spoofing examples

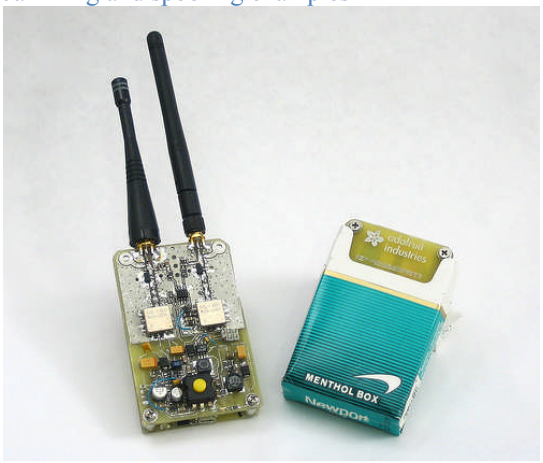

Figure 1. Compact mobile phone jammer2 (image from [3])

GSM-R

GSM-R is part of the European Train Management System (ERTMS) [4]. GSM-R is an adaptation of the GSM mobile telephone system standard to provide data and voice communications to trains. As some of the data is safety critical, the train must stop if the GSM-R connection is lost [5]. Compact battery powered Jammers can be purchased online for GSM systems and it is likely they can be successfully operated from within the train [6]. One mitigation for such attacks is the successful detection of the attack which can be achieved with a suitable channel monitoring system such as described in [7].

Radar

The jamming of radar systems has been used in electronic warfare almost since the invention of radar [8]. As well as their use for aircraft and shipping navigation and collision avoidance, radar systems are becoming more widely used in road vehicle safety systems and for autonomous vehicles.

GPS

GPS signals are very low level and easy to jam. It has been reported that criminals use GPS jammers to defeat vehicle tracking systems to enable the theft and hijacking of vehicles and their loads [9]. Feeding false information to (spoofing) a GPS system has been demonstrated on a number of occasions [10], [11]. With the increasing reliance on GPS for navigation in manned and unmanned vehicles, GPS spoofing opens many possibilities for hijacking and misdirecting a vehicle. Countermeasures which include the use of local sensors [12] and message authentication [13] are in development.

Wifi, M2M and other wireless data systems

In homes and offices we increasingly rely on wifi to allow mobile devices, smart TVs, security systems, and other household devices to communicate. In industry and commerce, machine to machine communications and sensor networks are increasingly used in daily operations. Whilst most of these systems can be reasonably robust against spoofing if suitable security measures are taken [14] there seem to exist a number of attacks which allow weak passwords to be cracked [15]. Recent hacking of connected vehicles has shown that many functions including engine and braking can be remotely controlled [16].

INTERFERENCE WITH ELECTRONIC SYSTEMS

Electronic systems in the UK undergo a degree of testing to meet the requirements of the EU Directive on Electromagnetic Compatibility [17] and are tested to standards which require them to have a degree of immunity to radiated and conducted electromagnetic interference. Typically, EMC standards require radiated immunity levels of a few volts per meter for electronic devices. This was intended to protect them from the fields generated by nearby wireless devices. Similarly, some immunity to conducted interference including electrostatic discharge and fast transient burst is required by EMC standards. These are again intended to ensure that the equipment operates successfully in a normal electromagnetic environment.

Currently portable electromagnetic weapons are readily available that are capable of radiating electric fields of tens to hundreds of kilovolts per metre at distances of a few metres to a few tens of metres [18], [19]. Similar pulse generators may be used to couple energy to power or signal cables that may be accessible.

IEMI Effects on electronic circuits

Interfering signals coupled into electronic circuits can cause a number of effects.

Demodulation

At low levels radio frequency interference signals, above the normal operating frequency range of the circuit can be demodulated by the non-linear elements in the circuit to produce a baseband signal which will interfere with any wanted signal (see Figure 2). Such behaviour will cause incorrect analogue voltage levels. Whilst digital circuits may be more immune to this type of experience it may still cause bit errors and jitter in signal timing resulting in incorrect operation of clocked circuits [20].

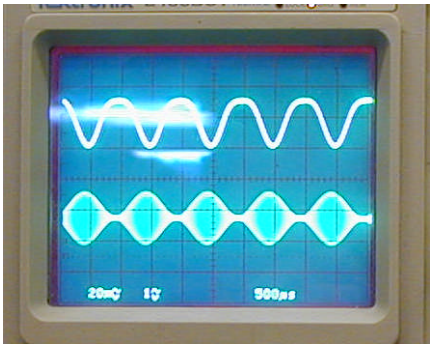

Figure 2. Output of an op-amp (top) when a 10MHz modulated sinusoidal signal (bottom) is injected into the inverting input .

Direct interference

Interfering signals within the passband of an electronic circuit will add directly to the existing signals and may affect the operation of circuits in a similar manner to demodulated signals.

Figure 3. IEMI Damage resulting in the destruction of a surface mount capacitor (Image courtesy of Metatech Corp).

Damage

As the amount of energy entering the system due to interference increases, there will eventually be enough heating of components to cause thermal damage, the effect is dependent upon pulse duration and magnitude and the size of the component where the energy is

dissipated [21]. Figure 3. and Figure 4. Show examples of damage to a capacitor and an IC due to IEMI.

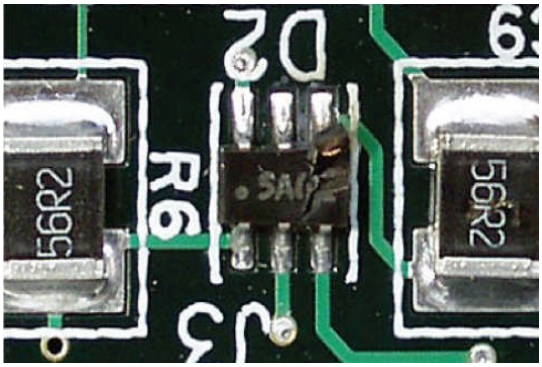

Figure 4. IEMI Damage resulting in the destruction of an IC (Image courtesy of Metatech Corp)

Examples of IEMI effects

A wide range of examples of EMC problems is given in the "Banana skins" series [22]. Some specific examples of Intentional electromagnetic interference are given, but many of the accidental cases could also be triggered by intentional interference. Sabath [23] describes a number of documented IEMI attacks on gaming machines, security systems, communications systems, and IT systems.

Immunity of IT systems

The susceptibility of Personal computers to EMI has been tested by a number of investigators. Hoad, Carter and Watkins [24] examined a number of computers under pulsed CW (30µs pulse with a prf of 1 kHz) interference in a reverberation chamber. When the "upset threshold" was measured All of the computers tested showed an increase in immunity with frequency and the more recent models (Pentium 4 processor) showed a better immunity than older (486 processor). The older (486) PCs experienced upsets at 90 V/m at 400 MHz rising to 2 kV/m at 8 GHz, whereas for the Pentium based models the upset levels were 500 V/m and 6 kV/m at the same frequencies. Whilst no definitive reason is given for the differences, it is suggested that with the advent of the EU directive on EMC, and increased processor speeds the manufacturers had to increase the shielding effectiveness of the case and pay more attention to the PCB layouts in order to ensure the radiated emissions standards were met. This also resulted in increased immunity. As ICs get faster with smaller transistors one might expect their susceptibility would decrease and the frequencies at which they are susceptible to increase. We have also observed that susceptibility tends to decrease with frequency in analogue ICs [25] until enough energy is injected to do physical damage.

Camp, and Garbe [26] tested the susceptibility of PC motherboards with no shielding to short pulse interference which showed that newer generations of motherboard were more susceptible to the pulsed interference than older generations. With 2.5 ns pulses they found that 486 based motherboards had a failure threshold of about 12 kV/m whereas a Pentium 3 based motherboard has a failure threshold of about 3 kV/m. Note that these fields are higher than some of the CW fields used by Hoad et al [24] even without the effect of case shielding. Short pulses need a higher amplitude to have an effect than CW waveforms or longer pulses [21]. Nitch et al [27] show similar effects and levels for a range of digital devices.

Kreitlow, Sabath, and Garbe [28] recently investigated the effects of IEMI pulsed sources on a small office IT network using a Diehl suitcase generator [29] which produces a damped sinusoidal waveform. In this scenario pickup on network cabling was expected to be a significant effect and with test fields of 5 kV/m induced common mode currents of 5 A were observed on the network cables. Whilst the interference was observed to cause some reduction of data transmission rates in the network, this was ameliorated by the network protocols and no upset to the system as a whole occurred. Brauer [30] applied short pulse (44 kV/m), damped sinusoidal (60 kV/m) and pulsed sinusoidal (70 kV/m) sources to network equipment and observed substantial reductions in network performance. The IEEE standard 1642-2015 [31] provides a recommended practice for IT equipment.

Whilst IT systems are often thought of in the office environment it must be remembered that they also make up the infrastructure which controls our factories, banks, power stations, and other critical infrastructure. Radasky and Savage describe effects of conducted and radiated interference on electric power systems in [32]. Parfenov et al [33] have shown that equipment power supplies are vulnerable to conducted transients which can propagate some distance on power lines in a range of scenarios.

Immunity of road vehicles

Most modern road vehicles rely on electronic engine management systems and these are vulnerable to IEMI. A commercial system is available to stop road vehicles using IEMI [34].

CONCLUSIONS

A brief review of the effects of IEMI on electronic systems, taken from the literature, has been presented which illustrate some of the possible effects. It can be seen from the examples that whilst many modern systems exhibit quite high levels of immunity, well above that required by EMC standards, IEMI sources are available that my cause temporary or permanent failures and this should be considered as a risk in the design of any critical systems. Radio, radar and GPS systems are particularly sensitive to low powered interference sources though some countermeasures are available to detect interference or spoofing.

Online version

This paper will be available online at https://www.researchgate.net/profile/John_Dawson9/publications after the EMC UK conference.

REFERENCES

[1] Wikipedia, "Cyber-physical system — Wikipedia, The Free Encyclopedia." 2015 [Online]. At: https://en.wikipedia.org/w/index.php?title=Cyber-physical_system&oldid=672867377

[2] W. A. Radasky and M. Backstrom, "Brief historical review and bibliography for Intentional Electromagnetic Interference (IEMI)," *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*, Aug. 2014 [Online]. At: http://dx.doi.org/10.1109/URSIGASS.2014.6929517

[3] L. Fried, "Wave Bubble: A design for a self-tuning portable RF jammer." 2011 [Online]. At: http://www.ladyada.net/make/wavebubble/index.html

[4] "The European Railway Traffic Management System (ERTMS)." [Online]. At: http://www.ertms.net/

[5] S. Dudoyer, V. Deniau, R. R. Adriano, M. N. B. Slimen, J. Rioult, B. Meyniel, and M. Berbineau, "Study of the Susceptibility of the GSM-R Communications Face to the Electromagnetic Interferences of the Rail Environment," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 54, pp. 667–676, Jun. 2012.

[6] M. Heddebaut, V. Deniau, S. Mili, J. P. Ghys, D. Sodoyer, and S. Ambellouis, "EM attacks on railway critical infrastructures," in *Proc. of the 2013 International Symposium on Electromagnetic Compatibility (EMC Europe 2013)*, 2013.

[7] M. Heddebaut, V. Deniau, J. Rioult, and G. Copin, "Method for detecting jamming signals superimposed on a radio communication: Application to the surveillance of railway environments," in *EMC Europe 2015*, 2015, pp. 1089–1094.

[8] M. Skolnik, *Radar Handbook, Third Edition*. McGraw-Hill Education, 2008 [Online]. At: https://books.google.co.uk/books?id=tA-KAwAAQBAJ

[9] "Conveyance Security Exposure GPS Jamming Devices and Unmanifested Cargo Introduction," Customs-Trade Partnership Against Terrorism, 2014 [Online]. At: http://www.cbp.gov/sites/default/files/documents/C-TPAT%20Alert%20-%20GPS%20Jamming%20Devices%20-%20October%202014.pdf

[10] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," *Journal of Field Robotics*, vol. 31, pp. 617–636, 2014 [Online]. At: http://radionavlab.ae.utexas.edu/publications/337-unmanned-aircraft-capture-and-control-via-gps-spoofing

[11] D. Mansson, R. Thottappillil, T. Nilsson, O. Lunden, and M. Backstrom, "Susceptibility of Civilian GPS Receivers to Electromagnetic Radiation," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 50, pp. 434–437, 2008.

[12] J.-H. Lee, K.-C. Kwon, D.-S. An, and D.-S. Shim, "GPS spoofing detection using accelerometers and performance analysis with probability of detection," *International Journal of Control, Automation and Systems*, vol. 13, pp. 951–959, 2015 [Online]. At: http://dx.doi.org/10.1007/s12555-014-0347-2

[13] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil GPS navigation message authentication," in *Position, Location and Navigation Symposium - PLANS 2014, 2014 IEEE/ION*, 2014, pp. 262–269 [Online]. At: http://radionavlab.ae.utexas.edu/publications/360-a-blueprint-for-civil-gps-navigation-message-authentication

[14] L. Buttyán and L. Dóra, "WiFi Security–WEP and 802.11 i," *EURASIP Jthisnal on Wireless Communication and Networking*, pp. 1–13, 2006 [Online]. At: http://www.hit.bme.hu/ buttyan/publications/ButtyanD06ht-en.pdf

[15] B. Antoniewicz, "802.11 Attacks," 2010 [Online]. At: http://www.mcafee.com/tw/resources/white-papers/foundstone/wp-80211-attacks.pdf?view=legacy

[16] A. Greenberg, "Hackers remotely kill a jeep on the highway—with me in it." Wired, Jul-2015 [Online]. At: http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[17] *Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast)*. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, [Online]. At: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0030

[18] D. V. Giri and F. M. Tesche, "Classification of intentional electromagnetic environments (IEME)," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 46, pp. 322–328, 2004.

[19] "EMP Suitcase: MIL-STD 464C Source" [Online]. At: http://www.apelc.com/wp-content/uploads/EMP-Suitcase_MIL-STD-464C-Source_PRODUCT-DATA-SHEET.pdf

[20] I. D. Flintoft, M. P. Robinson, K. Fischer, and A. C. Marvin, "Correlation of timing jitter and the re-emission spectrum in radiated immunity testing of digital hardware," in *Electromagnetic Compatibility, 2001. EMC. 2001 IEEE*

International Symposium on, 2001, vol. 1, pp. 541–546 vol.1.

[21] D. C. Wunsch and R. R. Bell, "Determination of Threshold Failure Levels of Semiconductor Diodes and Transistors Due to Pulse Voltages," *Nuclear Science, IEEE Transactions on*, vol. 15, pp. 244–259, 1968.

[22] K. Armstrong and A. E. Hutley, "The first 855 "Banana Skins." Oct-2014 [Online]. At: http://www.nutwooduk.co.uk/pdf/banana%20skins.pdf

[23] F. Sabath, "What can be learned from documented Intentional Electromagnetic Interference (IEMI) Attacks?," in *Proceedings of XXXth URSI General Assembly, Istanbul, Turkey, 13-20 August 2011*, 2011 [Online]. At: http://www.ursi.org/proceedings/procGA11/ursi/E03-9.pdf

[24] R. Hoad, N. J. Carter, D. Herke, and S. P. Watkins, "Trends in EM susceptibility of IT equipment," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, pp. 390–395, 2004.

[25] N. L. Whyman and J. F. Dawson, "Two level, in-band/out-of-band modelling RF interference effects in integrated circuits and electronic systems," in *Electromagnetic Compatibility, 1999. EMC York 99. International Conference and Exhibition on (Conf. Publ. No. 464)*, 1999, pp. 135–140.

[26] M. Camp and H. Garbe, "Susceptibility of Personal Computer Systems to Fast Transient Electromagnetic Pulses," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 48, pp. 829–833, Nov. 2006.

[27] D. Nitsch, M. Camp, F. Sabath, J. L. ter Haseborg, and H. Garbe, "Susceptibility of some electronic equipment to HPEM threats," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 46, pp. 380–389, 2004.

[28] M. Kreitlow, F. Sabath, and H. Garbe, "Analysis of IEMI Effects on a Computer Network in a Realistic Environment," in *EMC Europe 2015*, 2015, pp. 1063–1067.

[29] "HPEMcase: Non-Lethal Effector Systems for the Protection of Persons and Buildings," Diehl BGT Defence [Online]. At: http://www.diehl.com/en/diehl-defence/products/sensor-and-security-systems/protection-systems/convoy-protection.html

[30] F. Brauer, S. Fahlbusch, J. L. ter Haseborg, and S. Potthast, "Investigation of Hardening Measures for IT Equipment against Radiated and Conducted IEMI," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 54, pp. 1055–1065, Oct. 2012.

[31] "IEEE Recommended Practice for Protecting Publicly Accessible Computer Systems from Intentional Electromagnetic Interference (IEMI)," *IEEE Std 1642-2015*, pp. 1–39, Feb. 2015.

[32] W. Radasky and E. Savage, "Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid," Metatech Corporation, 358 S. Fairview Ave., Suite E, Goleta, CA 93117, Meta-R-323, Jan. 2010 [Online]. At: http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity/ferc_meta-r-323.pdf

[33] Y. V. Parfenov, L. N. Zdoukhov, W. A. Radasky, and M. Ianoz, "Conducted IEMI threats for commercial buildings," *Electromagnetic Compatibility, IEEE Transactions on*, vol. 46, pp. 404–411, 2004.

[34] "HPEMcarStop Non-violent system for selective stopping of vehicles in dynamic scenarios," Diehl BGT Defence [Online]. At: http://www.diehl.com/en/diehl-defence/products/sensor-and-security-systems/protection-systems/convoy-protection.html

Acknowledgement

The research leading to these results has supported by the Project STRUCTURES co-funded by the European Union Seventh Framework Programme under grant agreement n° 285257.

This is an updated postprint of: Dawson, J. F. , "Intentional Electromagnetic Interference Effects in Cyber-Physical Systems" , Proceedings of EMC UK 2015, 190-194, October 6-7 2015. invited paper